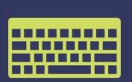
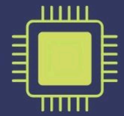
APUNTES SOBRE

DELITOS INFORMÁTICOS EN URUGUAY





M. Jackson - F. Scrollini

Mayo 2020

Este trabajo fue realizado como parte de un proyecto financiado por la Fundación para la Sociedad Abierta (Open Society Foundation), el mismo es publicado bajo una licencia Creative Commons 4.0 de Atribución. Para ver una copia de esta licencia, visite: http://creativecommons.org/licenses/by/4.0.

PREFACIO

Allá por el año 2016, con un grupo de colegas y el apoyo de la Fundación para la Sociedad Abierta, formamos lo que dimos a llamar DATYSOC, el Laboratorio de Datos y Sociedad. Se trataba de un equipo interdisciplinario de profesionales interesados en promover un marco de referencia sobre la situación de los derechos humanos en la era digital en Uruguay. Nos propusimos mover el escenario de estudios sobre tecnología y ciencias sociales en el medio local, y en mayor o menor medida lo logramos.

Este informe nació en ese marco y se desarrolló durante aquél 2016 y comienzos del 2017 a través de una serie de lecturas, entrevistas y eventos sobre el estado de la persecución de delitos informáticos en Uruguay.[1] Percibíamos cómo se acumulaban desde diferentes trincheras propuestas regulatorias y proyectos de ley que intentaban abordar este fenómeno. Ello nos motivó a realizar esta investigación, pretendiendo brindar insumos para entender mejor por qué y cuándo utilizar el derecho penal para acciones vinculadas a la tecnología.

Los caminos académicos y profesionales llevaron a que el informe estuviera durante muchos años acumulando polvo en algún disco duro. Aprovechando el encierro provocado por el COVID-19 es que hoy, tres años después, decidimos hacer públicos sus resultados.

---

[1] Agradecemos a los entrevistados que generosamente nos brindaron su tiempo y perspectivas sobre el estado de la seguridad digital en Uruguay. En virtud del largo periodo que ha transcurrido desde sus entrevistas hemos preferido por mantener sus nombres bajo reserva.

Lejos de ser un trabajo finalizado, podría ser considerado una versión *alfa* adaptada para reflejar los hallazgos que pueden resultar de utilidad aún cuando ha pasado tanto tiempo. Uno de los problemas identificados en el transcurso del trabajo fue justamente la falta de estudios en nuestro país que tomen perspectiva amplia del fenómeno de la delincuencia informática. Entendemos que la sola promulgación de una ley de delitos no era, ni es, la solución a un problema tan complejo. En este sentido nos propusimos aportar a la discusión a través del mapeo de la situación a nivel nacional y la conceptualización del impacto que pueden tener las normas de delitos informáticos en los derechos humanos.

A grandes rasgos, la legislación en este campo se mantiene incambiada lo que hace suponer que podría haber nuevos empujes normativos en cualquier momento. Apostamos a que la publicidad de estas líneas pueda servir de insumo a estudios más profundos y la búsqueda de mejores soluciones que incorporen la óptica de los derechos humanos. Si lo logramos la espera habrá valido la pena y desempolvar un viejo archivo de computadora dará sus frutos.

Fabrizio Scrollini - Matías Jackson
Montevideo, Mayo 2020

ÍNDICE

1

INTRODUCCIÓN

Uruguay ha destacado en los últimos 10 años por sus avances en materia de Tecnologías de la Información y Comunicación (TICs). La creación de una Agencia de Gobierno Electrónico (AGESIC), la implementación del Plan Ceibal (Programa One Laptop Per Child), campañas de concientización digital, la promulgación de una Ley de Protección de Datos Personales, la creación del CERTuy, así como muchas otras medidas han llevado a Uruguay a obtener menciones especiales, premios y primeros lugares en los rankings especializados en Sociedad de la Información. Así, por ejemplo, en el E-Government Survey 2016 de Naciones Unidas, Uruguay ocupa el primer lugar en Sudamérica y tercero en toda América, sólo precedido por Estados Unidos y Canadá (ONU, 2016). Todo demuestra el especial interés del país por constituir su marca "Uruguay Digital".

Sin embargo, existe una categoría en las mediciones por la que Uruguay no destaca: la tipificación e investigación de delitos informáticos.

Según el informe "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?", Uruguay no logra superar el nivel "Formativo" de madurez en lo que refiere a delincuencia cibernética, investigación jurídica y divulgación responsable de información, muy por debajo de su promedio general en el índice.

Según el Reporte: "La Unidad de Delitos Cibernéticos de la Policía Nacional es el organismo responsable de la investigación de los delitos cibernéticos. Recibe capacitación de la OEA y otras

organizaciones, y mantiene un laboratorio forense digital. En los últimos años la unidad ha detectado un aumento de la delincuencia cibernética. El Gobierno de Uruguay ha elaborado un marco jurídico para la seguridad cibernética y ha adoptado la Ley no 18.331 de Protección de Datos. Sin embargo no ha adoptado una legislación penal específica para los delitos informáticos y no cuenta con ningún mecanismo de divulgación para el sector privado."[2] (OEA, BID, 2016)

La falta de legislación específica en la materia es vista por los organismos internacionales como una desventaja a la hora de luchar contra los criminales que ejecutan sus actos a través de la red. Al tratarse de un fenómeno internacional, afirman, resulta fundamental la armonización y coordinación de las diferentes jurisdicciones.

En el mundo existen numerosos intentos de regulación que han sido criticados por su avasallamiento a las libertades individuales, las potestades transfronterizas de persecución y por buscar controlar los contenidos que circulan a través de Internet. En este sentido, leyes como la de Pakistán o Nigeria han sido duramente criticadas por organizaciones internacionales abocadas a la defensa de los derechos digitales (Reuters, 2016)

En la región latinoamericana, se destaca el caso peruano, que en 2013 aprobó su ley de delitos informáticos, la cual fue duramente cuestionada por la sociedad civil de dicho país por su redacción amplia y ambigua, que permitía criminalizar conductas como el Hacking Ético o el simple borrado de archivos. (La República Perú, 2013) Poco tiempo después la norma fue modificada adoptando una redacción más acotada y dentro de los parámetros del Convenio de Cibercrimen de Europa. El ejemplo de Perú demuestra la necesidad de conocer efectivamente las

[2] Los datos para la elaboración de la medición en Uruguay fueron brindados por AGESIC, ANTEL y el Ministerio de Defensa.

conductas que se están regulando y los efectos que esto puede acarrear.

En Uruguay, a iniciativa de varios partidos políticos se han presentado al Poder Legislativo diferentes proyectos de tipificación de delitos informáticos. Algunos de estos proyectos resultan más amplios que otros, aunque ninguno ha pasado más allá del debate parlamentario.

La promulgación de una ley penal que criminalice determinadas conductas vinculadas a las tecnologías de la información puede poner en riesgo el ejercicio de diferentes derechos humanos. Por ejemplo, del derecho a buscar y recibir información se desprende el derecho de los usuarios a conocer y auditar los sistemas tecnológicos que utilizan y en los cuales, cada vez más, confían sus datos personales. Penalizar conductas que busquen la investigación y el acceso al conocimiento puede representar un obstáculo al desarrollo y mejora de la propia seguridad informática que se busca proteger.

El propósito del presente trabajo es realizar un análisis descriptivo del estado de situación de la regulación e investigación de los delitos informáticos en Uruguay. Se busca a través de ello aportar información que guíe la toma de decisiones y contribuya al debate público en la materia. La creación de nuevos tipos penales debe realizarse bajo determinados cuidados y teniendo en cuenta los principios de lesividad, intervención mínima y proporcionalidad de la pena.

Es por ello que el abordaje realizado toma como referencia el marco internacional de derechos humanos y el principal tratado referido a delitos informáticos, el Convenio de Cibercrimen del Consejo de Europa. Durante todo el trabajo se procurará tener un abordaje práctico de la materia para así conocer el estado actual

de situación respecto a la prevención, persecución y represión de los delitos informáticos.

El trabajo se encuentra dividido en tres partes. En primer lugar, se realiza una descripción de la situación en Uruguay buscando contestar tres preguntas:

1. ¿Cuáles son los organismos públicos que intervienen en la persecución de los delitos informáticos?;

2. ¿Quiénes son los sujetos que realizan este tipo de actividades?; y

3. ¿Cuál es el marco legal vigente?

En segundo lugar, se realiza un análisis de los principales delitos reconocidos como ‘delitos informáticos’. Para esto se tomará como referencia el Convenio de Ciberdelincuencia de la Unión Europea. Se procura señalar las diferentes modalidades y conductas que podrían quedar englobadas dentro de cada uno de los tipos penales dependiendo del mayor o menor alcance que se pretenda dar a las normas. Asimismo nos valemos de la experiencia en el derecho comparado y las referencias a nivel nacional a través de la jurisprudencia de los Tribunales Penales de forma tal de conocer cuáles son los instrumentos de los que jueces y fiscales se valen hoy en día.

En tercer lugar, se hace referencia a la fase procesal de investigación y persecución de los delitos. Se indican las implicancias que la persecución penal puede tener sobre la vulneración de derechos individuales.

Por último, se brindan recomendaciones para la redacción de una ley de delitos informáticos como parte fundamental de una política integral de seguridad digital.

2

DELITOS INFORMÁTICOS Y DERECHOS HUMANOS

Marco Internacional de Derechos Humanos

La introducción de nuevos tipos penales al ordenamiento jurídico debe ser parte de un análisis global y sistemático que tenga en cuenta la importancia de los derechos en juego. Para ello se recomienda tener presente el marco internacional en materia de Derechos Humanos ratificado por Uruguay, teniendo una visión integradora que comprenda la tecnología como una herramienta de empoderamiento social.

En el nuevo escenario que las TIC's y en especial Internet plantean, cobran especial importancia los Derechos a la Libertad de Expresión y la Privacidad. Ambos derechos se encuentran amparados en los instrumentos internacionales y sirven de base para el análisis aquí realizado sobre los proyectos legislativos de delitos informáticos.

La **Declaración Universal de Derechos Humanos (DUDH)**, reconoce en su artículo 19, el Derecho de todo individuo a la

libertad de opinión y de expresión. Este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. Asimismo, el artículo 12 garantiza la protección legal contra injerencias arbitrarias en la vida privada, familia, domicilio y correspondencia.

El **Pacto Internacional de Derechos Civiles y Políticos (PIDCP)**, ratificado en nuestro país por la Ley 13.751, protege estos derechos en sus artículos 17 y 19. La **Observación General No. 34** del Comité de Derechos Humanos de la ONU reconoce expresamente la vital importancia que adquiere el artículo 19 del PIDCP en Internet.

A nivel regional, la Convención Americana de Derechos Humanos ratificada en nuestro país por la Ley 15.737, del 8 marzo de 1985, otorga fundamental importancia a la libre circulación de información e ideas, cuyas restricciones deben ser mínimas y excepcionales (Art. 13). La dignidad y privacidad se encuentran protegidos por el artículo 11 de la Convención.

En el año 2011 los Relatores Especiales para la Libertad de Expresión de ONU, OEA, OSCE y CADHP, se pronunciaron mediante la **Declaración Conjunta Sobre Libertad De Expresión e Internet,** dejando en claro que "Las restricciones a la libertad de expresión en Internet solo resultan aceptables cuando cumplen con los estándares internacionales que disponen, entre otras cosas, que deberán estar previstas por la ley y perseguir una finalidad legítima reconocida por el derecho internacional y ser necesarias para alcanzar dicha finalidad (la prueba 'tripartita')".

Convenio de Budapest

El documento de referencia en la materia a nivel internacional es el Convenio sobre la Ciberdelincuencia del 23 de noviembre de 2001 (En adelante Convenio de Budapest). El instrumento busca armonizar las legislaciones de los países signatarios estableciendo los delitos que deberán tipificar, adjudicando reglas de competencia y brindando herramientas de cooperación judicial. El Convenio se encuentra abierto para su ratificación, contando a 2016 con 50 adhesiones. En América, lo han ratificado Argentina, Chile, Colombia, Costa Rica, México, Panamá, Paraguay, Perú, República Dominicana y Estados Unidos.

El Convenio, único instrumento internacional vinculante en la materia, obliga a los Estados firmantes a adoptar legislación interna que castigue conductas referidas a la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos, al patrimonio, la pornografía Infantil, y propiedad intelectual. Incluye además previsiones sobre potestades de investigación conjunta entre países y herramientas de cooperación internacional.

Budapest se enfoca en las conductas criminales, no en las técnicas o tecnologías utilizadas por los atacantes. Si bien no se incluyen a texto expreso, la adopción de los tipos penales en él previstos permiten la persecución de redes de Botnets, ataques de denegación de servicios (DOS o DDOS), suplantación de identidad, phishing, uso de malware, y ataques a infraestructuras críticas de información. (Consejo de Europa, 2014)

A pesar de ser el documento que ha marcado el camino a nivel internacional, el Convenio no está exento de defectos o mejoras a realizar. Una de las principales críticas que se realizan sobre Budapest es su desbalance a favor de la seguridad por sobre las garantías de protección de los derechos humanos.

En este sentido la dinámica de Budapest ha sido acertadamente reseñada de la siguiente manera: Elevar los niveles de seguridad es un imperativo que requiere reglas comunes internacionales, pero implementar garantías es competencia nacional que debe ser negociada, teniendo en consideración los pactos internacionales de Derechos Humanos. (Hosein & Yalamova, 2013)

Algunos países han manifestado su oposición a ratificar un Convenio en el cual no fueron parte de ninguna negociación. Además disposiciones procesales sobre la Orden de presentación de información a autoridades extranjeras (Art. 18) o el Acceso transfronterizo a Datos (Art. 32 lit. B) son a menudo considerados insuficientes para proveer una cooperación judicial acorde a los estándares de Derechos Humanos. (de La Chapelle & Fehlinger, 2016)

A pesar de estas críticas, el Convenio mantiene su posición como referencia en la materia. Una de las mayores virtudes del Convenio de Budapest, y la razón principal por la que el Convenio sigue siendo el marco de referencia aún 16 años después de su aprobación, en un ambiente que ha cambiado tanto como es Internet, se debe a la neutralidad de su redacción, por la cual no se apegó a ninguna tecnología existente al momento, sino que es lo suficientemente abierto como para adaptarse a los cambios que las TICs provocan.

3

SITUACIÓN NORMATIVA E INSTITUCIONAL

La respuesta que los países han dado a nivel nacional frente al fenómeno de la ciberdelincuencia abarca diferentes medidas, siendo la tipificación de delitos sólo una de ellas. La Unión Internacional de Comunicaciones reconoce cinco pilares en los que gobiernos y demás actores deben trabajar en conjunto para lograr avances en la ciberseguridad: Medidas jurídicas, medidas técnicas, medidas organizativas, creación de capacidades y cooperación internacional.[3] (UIT, 2014)

Como indican las organizaciones internacionales y la experiencia comparada, el combate al cibercrimen no se realiza únicamente mediante la aprobación de leyes penales con nuevos delitos adaptados a la era de Internet sino que requiere un análisis integral de la situación, conocer las prácticas, sus efectos, los actores involucrados y los procedimientos llevados a cabo para la investigación y persecución de los delincuentes.

---

[3] Teniendo en cuenta los diferentes factores que operan en estas cinco áreas, la UIT coloca a Uruguay en el puesto número 8 del ranking mundial de preparación y compromiso con la ciberseguridad, compartiendo la posición con Hong Kong, Finlandia, Qatar y Eslovaquia. (UIT, 2015)

Situación normativa

Uruguay no cuenta hoy con una Ley específica de Delitos Informáticos. Sin embargo, esto no quiere decir que no existan en nuestro ordenamiento jurídico algunos delitos que sí son considerados como informáticos, tanto por doctrina como por documentos internacionales en la materia.

La Ley 17.616 modificatoria de la Ley de Derechos de Autor de 1937 introdujo dentro de los bienes protegidos a texto expreso los programas de ordenador y las bases de datos. El artículo 46 prevé una serie de conductas castigadas penalmente por contravenir la protección de derechos autorales, cuando se realicen "por cualquier medio".[4]

La Ley 17.815 de Violencia Sexual contra Niños, Adolescentes o Incapaces tipificó la fabricación, producción, comercio, difusión y facilitamiento, en cualquier medio, de material pornográfico con menores de edad o incapaces.

La Ley 18.383 del 2008 modificó el artículo 217 del Código Penal para tipificar el delito de Atentado contra la regularidad de las telecomunicaciones alámbricas o inalámbricas, castigándolo con una pena de tres meses de prisión a tres años de penitenciaría.

El artículo 4 de la Ley 18.600 de Documento y Firma Electrónica establece que: "El que voluntariamente transmitiere un texto del que resulte un documento infiel, adultere o destruya un documento electrónico, incurrirá en los delitos previstos por los artículos 236 a 245 del Código Penal, según corresponda." Es decir que, para evitar que los Jueces recurran a analogías in

[4] Varias organizaciones de la Sociedad Civil apoyan la modificación de la legislación vigente a través del proyecto de reforma que se encuentra a estudio en el Parlamento. Más información: http://www.todosganamosderechos.org

malam partem, el legislador optó por equiparar el documento electrónico al papel, y de esta manera hacer aplicable a los nuevos medios el capítulo de Falsificación Documentaria del Código Penal.

Desde la adopción del Convenio de Budapest a nivel internacional a la fecha, han existido en Uruguay tres proyectos legislativos en la materia. El primero de ellos fue presentado por el Senador Tabaré Viera en el año 2010 y buscaba introducir los delitos referidos en el Convenio de Budapest que aún no se encontraban tipificados por nuestro ordenamiento jurídico. En el año 2014, AGESIC a través del Poder Ejecutivo presentó su propio proyecto, el cual también fue archivado. En 2016 se presentó a estudio de la Comisión de Innovación, Ciencia y Tecnología de la Cámara de Diputados un nuevo proyecto, presentado en Mayo de ese mismo año también por el Senador Tabaré Viera con una redacción diferente a la presentada en el 2010. A estos tres proyectos se pueden sumar las iniciativas del Senador Pedro Bordaberry presentadas en Marzo de 2015 para agregar al Código Penal los delitos de: Pornografía de Venganza, Robo de Identidad y Ciberacoso contra menores de edad. Como evidencian los múltiples proyectos legislativos presentados, la tipificación de conductas criminales mediante el uso de computadoras está latente en nuestro sistema político.

Situación institucional

Desde el año 2012, el Ministerio del Interior cuenta con un Departamento especializado en Delitos Informáticos. Esta oficina se encarga de llevar adelante las investigaciones en las que la tecnología se utilizó como medio para cometer el delito.

Además de la Oficina de Delitos Tecnológicos, la Administración se completa con los Centros de Respuesta a

Incidentes Informáticos, que en nuestro país son dos: El CertUY y el DCSIRT.

El artículo 73 de la Ley de Rendición de Cuentas del Ejercicio 2007, Número 18.362, creó dentro del ámbito de AGESIC al Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy) con el objetivo de regular la protección de los activos de información críticos del Estado. De la normativa mencionada surgen los siguientes cometidos del CERTuy:

- Difusión de las mejores prácticas en el tema.

- Centralizar, coordinar la respuesta a incidentes informáticos y realizar las tareas preventivas que correspondan.

- Asesorar en la definición de políticas, metodologías y buenas prácticas en seguridad de la información en la Administración Pública.

- Brindar apoyo en las etapas de implementación de estas políticas.

Por su parte, el Ministerio de Defensa también cuenta con su Centro de Respuestas, denominado D-CSIRT. Creado por el artículo 73 de la Ley N° 18.362 y reglamentado por el Decreto 36/2015, el D-CSIRT es el encargado de coordinar las actividades relacionadas a incidentes de seguridad de la información dentro de todo el Ministerio de Defensa.

Los tres órganos (Delitos Tecnológicos, CertUY y DCSIRT) son parte de redes regionales e internacionales de intercambio de información. Entre ellas trabajan de forma coordinada aunque sin un espacio formal de cooperación. Se están llevando adelante esfuerzos para formalizar protocolos que mejoren el intercambio de información entre las tres oficinas.

Según los estándares internacionales, la información referente a la Seguridad Pública reviste un alto interés público, siendo la regla de principio la transparencia y la excepción su reserva. Existen en este sentido dos esfuerzos globales para identificar una serie de principios que permitan armonizar el derecho a saber con los intereses de seguridad nacional: los "Principios de Johanesburgo" elaborados por la organización Artículo XIX, y "Principios sobre seguridad nacional y el derecho a la información", elaborados por la Open Society Justice Iniciative. (Bertoni, et al., 2012)

La información estadística reviste en el campo de los delitos informáticos un activo imprescindible para conocer cuáles son las conductas socialmente reprochables y que merecen un castigo penal. Los informes anuales del Observatorio Nacional sobre Violencia y Criminalidad no discriminan datos sobre delitos informáticos o que tuvieran un componente tecnológico en su ejecución. Por su lado, el CertUy publica anualmente desde el 2014 las estadísticas, en las cuales se indican las maniobras técnicas más utilizadas en los incidentes de seguridad reportados.[5]

Como parte de esta investigación se realizó una solicitud de acceso a la información pública al Ministerio del Interior, al amparo de la Ley No. 18.381, buscando acceder a estadísticas de Delitos Informáticos en Uruguay, cantidad de denuncias efectuadas ante el Departamento de Delitos Informáticos de la Policía y cantidad de policías asignados a este Departamento. El día 16 de Agosto de 2016, el Ministerio del Interior contestó a la solicitud que luce en el Anexo del presente documento.

---

[5] Disponibles en: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/datos-y-estadisticas/estadisticas

4

DELITOS INFORMÁTICOS EN URUGUAY

Se analizan a continuación las conductas que usualmente son enmarcadas dentro de las regulaciones nacionales e internacionales de delitos informáticos. Para cada una de ellas se procuró analizar el fundamento de su castigo, los riesgos que puede suponer para el ejercicio de derechos humanos y la forma en que los Tribunales nacionales han atendido situaciones similares utilizando la legislación vigente.

Acceso ilícito

En la generalidad de los casos, el delito de acceso ilícito es asociado a la actividad de los Hackers de sombrero negro: Sujetos que con conocimientos avanzados en informática logran ingresar a un sistema y extraer información, dinero o modificarlo para sus propios intereses. Ya sea destruyendo datos, divulgándolos, vendiéndolos o alterándolos, estos especialistas explotan vulnerabilidades buscando el provecho personal. Es el estereotipo que se puede apreciar en artículos de prensa cuando se habla genéricamente de ‘hackers’.

A nivel doctrinario, el acceso sin otros fines o conductas dañosas, lo que se conoce como "mero intrusismo" es motivo de disputa debido al reconocimiento del bien jurídico que se pretende tutelar. Así hay quienes sostienen que estamos ante un nuevo bien jurídico merecedor de protección penal: La seguridad informática. Adquiriendo los conceptos propios de la Seguridad de la Información, estos autores entienden que los sistemas deben mantener el tríptico de Confidencialidad, Disponibilidad e Integridad. En la sociedad de la información, la confianza y el buen funcionamiento de los sistemas informáticos, constiuyen la base sobre la cual se edifica el entramado social y económico. En este contexto el intrusismo, aunque no genere daños o delitos posteriores, es razón suficiente para ver debilitada esa confianza y merecer su elevación como bien jurídico penalmente protegido.

Por otro lado, hay quienes entienden que las actividades de ingreso a un sistema sin autorizaciones no constituye por sí misma una conducta suceptible de ser reprochable penalmente. Afirman que el derecho ya cuenta con respuestas adecuadas cuando las conductas conducen a un daño a otro bien jurídico, como puede ser la intimidad, la seguridad económica, el daño de los datos, etc. La tipificación del acceso simple constituye un delito de peligro abstracto que atenta contra una proyección garantista y de derecho penal de mínima intervención.[6]

Los países desarrollados y organismos internacionales se han inclinado por la primera de estas dos opciones, eligiendo la tipificación específica de esta conducta. Ya en el año 1989, la Recomendación sobre Crímenes Relativos a Computadoras del Consejo de Europa, sugería la tipificación del Acceso Sin Autorización "pura y simple", es decir, sin más requisitos objetivos o subjetivos. Según el documento, el bien jurídico protegido era el "Domicilio informático" y con él se intenta poteger su integridad desde una etapa temprana para evitar

[6] Sobre el bien jurídico protegido ver (Matellanes Rodríguez, 2008)

conductas más dañinas como el daño informático o el espionaje. Una de las particularidades de esta Recomendación es la previsión opcional de conceder una especie de gratificación en la pena para aquellos autores del delito que dieran inmediata noticia del acceso o brecha de seguridad a la víctima o las autoridades competentes.

El Convenio de Budapest deja la puerta abierta para que además del acceso "doloso y sin autorización", el tipo penal pueda exigir: 1) Como elemento objetivo, la vulneración de medidas de seguridad (Como podrían ser los sistemas de protección DRM), o que el ataque sea sobre un sistema que se encuentre conectado a otro (A través de redes, o telemático); 2) Como elemento subjetivo, la intención de obtener datos informáticos, o con otra intención delictiva.

Para establecer la pena que corresponda a este delito, se deben tener en cuenta: 1) Que se trata del delito más leve, básico y de aplicación subsidiaria, y 2) La falta de consenso sobre la necesidad de su tipificación como delito autónomo cuando se podría recurrir al Derecho Civil o Administrativo. Teniendo en cuenta estos factores, el castigo debería encontrarse en los baremos más bajos cuando se produce el "simple intrusismo", sin otra finalidad u acción posterior.

Muchas veces, el acceso ilícito buscar obtener información de la víctima, ya sea persona, empresa u organismo público, para luego divulgarla públicamente. Cuando la divulgación refiere a información de un ente o empresa estatal, la regulación debería tener en cuenta si la misma reviste o no un interés público.[7] Esta valoración brindaría mayores protecciones a los denunciantes de actos de desviación de poder o 'whistleblowes', quienes son

---

[7] Apartándose de las previsiones del Convenio de Budapest, el Proyecto 2016 previó como agravantes especiales la difusión de la información obtenida mediante el acceso.

amparados por el Marco Interamericano de Derechos Humanos. (Organización de Estados Americanos, 2013)

El 24 de diciembre de 1998, el Tribunal de Apelaciones en lo Penal de 1º Turno dictó sentencia en el que podría considerarse como uno de los primeros casos judiciales en los que se estudia una conducta de acceso ilícito a un sistema.[8]

El imputado, una persona con estudios avanzados en informática y empleado del LATU, logró superar "por diversión" las barreras de seguridad informática del Laboratorio, ingresando a archivos a los que sólo tienen acceso los clientes. "Según se desprende del informe del perito de la Suprema Corte el encausado tenía los password del LATU y también el archivo shadow, con las claves de los usuarios del mismo. Y también un archivo con los pasos realizados para descifrar claves del citado laboratorio. Además de otros documentos nacionales y extranjeros obtenidos de la misma manera, que son propiedad exclusiva de sus titulares, y que sólo pueden acceder a ellos quienes están autorizados."

El Tribunal confirmó la sentencia de primera instancia por la cual se le tipificó el delito de Conocimiento fraudulento de documentos secretos. A juicio de los Magistrados, "desde que, un archivo (aun cuando no contenga "secretos") está protegido con una clave de seguridad, para aquel que no cuente con ella, es secreto o confidencial." El argumento de la defensa de considerar que la acción fue por diversión, o animus jocandi fue descartado "ya que no se explica por qué razón archivó los datos y sobre todo las claves de seguridad, que halló con un programa especial creado o no por él. Y si tenemos en cuenta, cuantos (sic) archivos violados tenía en su disco duro, el tal ánimo queda descartado".

---

[8] Sentencia Nº 234 del 24 de Diciembre de 1998 del Tribunal de Apelaciones en lo Penal de 1º Turno.

Interceptación ilícita

La interceptación de datos en las redes telemáticas funda su tipificación en los valores de privacidad e intimidad, que merecen su protección tanto en el mundo analógico como digital. Es ineludible su proximidad con la inviolabilidad de correspondencia, protegida por los Artículos 28 de la Constitución de la República y 297 del Código Penal.

Los Proyectos presentados ante el Parlamento se apartan, abarcando más conductas, que las recomendadas por el Convenio de Budapest; Se agregan en ellos interrumpir e impedir el flujo de datos.

Al momento de establecer la pena para este delito debería mantenerse la proporcionalidad con los delitos del 296 y 297 del Código Penal que van de 20 a 400 Unidades Reajustables de multa.

Daño Informático o Interferencia en los datos

El delito de Daño Informático, busca proteger la integridad, disponibilidad y seguridad de los datos almacenados en un sistema, por formar estos parte del patrimonio de una persona o por el valor económico que éstos puedan tener.

Hoy, se trata de uno de los delitos más populares debido a la explosión del Ransomware, un tipo de malware que bloquea mediante cifrado el acceso a los archivos de la víctima. A cambio de entregar la contraseña, los delincuentes solicitan grandes sumas de dinero.

La doctrina nacional señala que actualmente el delito de daño previsto en el artículo 358 del Código Penal no permite el castigo

del daño sobre datos informáticos debido a que la redacción se limita al daño sobre bienes muebles o inmuebles.[9] (Pecoy, 2012)

Algunos países han optado por incluir los datos informáticos dentro de las previsiones del Delito de Daños tradicional. Este es el caso de Argentina, donde la Ley 26.388 agregó el siguiente inciso al artículo 138 del Código Penal: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". En cambio, otros países como España y Colombia han optado por tipificar el delito de daño informático como un delito autónomo.

En cualquiera de las dos opciones, regulación en el mismo delito de daños o creando un tipo penal nuevo, resulta recomendable incluir como requisito objetivo que el daño provocado sea "grave", ratificando así el principio de lesividad y el carácter de última ratio del Derecho Penal. El Convenio de Budapest (Art. 4) prevé ésta posibilidad de manera que la Justicia Penal actúe únicamente frente a conductas de cierta entidad y que efectivamente dañen el bien jurídico tutelado. Para los daños de menor gravedad, el afectado podría recurrir a la vía civil de reparación patrimonial.

Existiendo además una correlación tan estrecha con el delito "clásico" de daño, las penas a establecer deberían mantener la correspondencia. El hecho de realizar estas conductas por medios informáticos no debe servir de justificación para castigar más duramente si el bien jurídico protegido es el mismo. Cualquier cambio en el baremo punitivo debería verse reflejado en la exposición de motivos, lo cual no ocurre en ninguno de los proyectos presentados al momento, los cuales aumentan

---

[9] Hoy sería únicamente perseguible el daño de datos que afecten la utilidad del bien material en el que se encuentran almacenados, por ejemplo suprimiendo el BIOS de una computadora provocando que ésta no encienda.

considerablemente la multa de entre 20 y 900 Unidades Reajustables prevista para el delito de daño en el Código Penal.

La falta de tipificación expresa del delito de daño informático no fue obstáculo para que el Tribunal de Apelaciones en lo Penal de 3º Turno ratificara la condena realizando una interpretación amplia del artículo 358 del Código Penal. "En referencia al agravio de la defensa que refiere al delito de daño debe considerarse que el encausado AA a fs. 78 y vta. admite el daño a la informática. Así, preguntado quien daño el sistema informático y qué fue lo que realmente se dañó o eliminó. Contesta: 'Fui yo, solo, eliminé los archivos a la parte correspondientes a padrones, a la parte permisos, expedientes y de consulta diaria. Lo que hice fue eliminar los datos'."[10]El Tribunal también entendió que al producirse el daño en un sistema perteneciente a la administración pública, era procedente aplicar la agravante del Artículo 359 Numeral 2.

Sabotaje informático

El Convenio de Budapest (Art. 5), prevé que la obstaculización al sistema tiene que ser "grave", es decir contar con cierta entidad que permita excluir la calificación delictual de atentados contra sistemas de menor importancia. Esta fue la opción adoptada por Alemania que en su tipo penal requiere que los datos interferidos fueran de "importancia sustancial" para el tercero afectado (Sección 303b Código Penal Aleman).

El verbo nuclear del delito previsto en el Proyecto 2016 es también "obstaculizar", pero sin el requisito de entidad grave, lo cual permitiría interpretaciones amplias y/o absurdas que abarcaría conductas casi insignificantes.

[10] Sentencia Nº 234 del 2008 del Tribunal de Apelaciones en lo Penal de 3º Turno.

Los encargados de redactar el Convenio de Budapest consideraron como "grave" el envío de datos a un sistema en particular cuando su forma, tamaño o frecuencia produzca un efecto perjudicial significativo en la capacidad que tiene el dueño o el operador para utilizar dicho sistema, o para comunicarse con otros sistemas (por ejemplo, por medio de programas que generen ataques de "denegación del servicio). (Consejo de Europa, s.f.)

En 2011, Uruguay fue objeto de una amenaza pública de parte del colectivo Anonymous, en la que se comunicó el ataque a sitios web oficiales mediante ataques de denegación de servicios distribuidos (DDOS). (Anon., 2011) De acuerdo al testimonio de los entrevistados, esta fue la situación de mayor riesgo hasta el momento, que se logró mitigar gracias a las medidas preventivas adoptadas.

Abuso de dispositivos

El Delito de Abuso de Dispositivos tiene como objetivo tipificar la producción, venta, importación o puesta a disposición de hardware, software o contraseñas que permitan la comisión de alguno de los delitos mencionados anteriormente. Se trata de un delito de peligro, por el cual se presume el carácter peligroso de los comportamientos para los datos y sistemas y se elevan a la categoría de delito autónomo conductas que constituyen, en realidad, actos preparatorios o tentativa del injusto previstos en los artículos anteriores. Se configura así como un delito de peligro cuya relevancia típica se ve colmada por la concurrencia del ánimo de causar daños sin que sea necesario que éstos se produzcan.

Al adelantar la acción penal a un momento previo a la efectiva producción del daño se debe ser cuidadoso de no abarcar conductas que no merezcan sanción alguna. Es el caso de las

herramientas que permiten un uso dual. Hoy las herramientas informáticas son sumamente versátiles permitiendo usos buenos, malos, legales e ilegales. Un mismo programa o dispositivo, en tanto herramienta, puede ser usado para distintos fines, por lo que castigar el uso o manipulación por el hecho de ser apto (aún potencialmente) para cometer un delito parece por demás excesivo capturando dentro de esta figura miles de programas o dispositivos que son usados diariamente por todos.

Se deben prever, al igual que lo hace el Convenio de Budapest la realización de pruebas autorizadas, como podrían ser las realizadas por hackers éticos que utilizan herramientas y software para testear la seguridad de los sistemas y así conocer sus vulnerabilidades.

Falsificación informática

La inclusión de delitos que castiguen la falsificación documentaria en el entorno digital busca eliminar cualquier tipo de vacío legal que pudiera dejar la regulación tradicional. Se protege así la seguridad jurídica, necesaria para garantizar el buen funcionamiento de los servicios en la sociedad de la información.

Desde el punto de vista penal, este escollo ya fue resuelto por nuestro legislador, que en el artículo 4 de la Ley 18.600 de Firma y Documento Electrónico expandió la aplicación de los Delitos de Falsificación Documentaria a los almacenados y transmitidos por medios electrónicos, haciendo totalmente innecesaria su inclusión en una nueva Ley Penal.

El Convenio de Budapest otorga el margen necesario para que los Estados exijan dentro del elemento subjetivo del tipo la intención de cometer otro delito para que exista responsabilidad por este artículo.

Una de las modalidades de operación que involucra la falsificación de documentos es el "phishing". Recientemente, en agosto de 2016 circuló un correo que simulaba provenir de la Dirección General Impositiva, y que escondía en su archivo adjunto un virus que disparaba una vulnerabilidad en el equipo de la víctima (Certuy, 2016). Lo mismo ocurrió con correos a nombre del Poder Judicial, donde se amenazaba a los destinatarios con el pago de una multa (Machado, 2014).

Fraude informático

La introducción de datos fraudulentos en el procesamiento informático con el fin de obtener un beneficio económico es una de las modalidades más antiguas de los ciberdelincuentes. El bien jurídico protegido en este tipo es el patrimonio económico de la persona. Así el Convenio de Budapest prevé que se castiguen los "actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona...".

La inclusión de este delito, acabaría con las discusiones doctrinarias sobre la aplicación de la Estafa a situaciones en que se actúa sobre un sistema informático, que diera lugar a la figura conocida como "Estafa Mecánica".

Uno de los casos más conocidos en nuestro país y que generó discusión a nivel doctrinario sobre la necesidad de tipificar nuevos delitos es el referido a la falsificación de tarjetas de teléfonos públicos. Según surge de las sentencias del caso, ANTEL presentó denuncia penal al constatar el funcionamiento irregular en diversas tarjetas de teléfonos. Desde estas tarjetas de valor $ 200, se llegaron a realizar llamadas por más de $ 370.000.

El Departamento de Delitos Económicos logró dar con tres sujetos que utilizando sus conocimientos en electrónica habían modificado el jumper de la tarjeta para lograr que el sistema no

comprobara el agotamiento del saldo. El Juez de Primera Instancia en lo Penal de 4º Turno los condenó como autores de un delito continuado de hurto de energía eléctrica, en el entendido de que “los teléfonos por cable funcionan a través de energía (más precisamente eléctrica), por lo cual los enjuiciados hurtaron la misma en perjuicio de ANTEL, que es la usuaria de la línea y propietaria del servicio que con ella se brinda, lo que ocasionó en su perjuicio el dejar de percibir el valor asignado a las llamadas...”

Tras la apelación de este primer pronunciamiento, el Tribunal de Apelaciones en lo Penal de 2º Turno, revocó y condenó por un delito continuado de estafa.[11] El Tribunal admite la existencia de la Estafa Mecánica en nuestro ordenamiento, donde la inducción al error se produce sobre el sistema electrónico e indirectamente sobre del Ente. La Suprema Corte de Justicia confirmó el fallo de segunda instancia.[12]

El mismo año, el Juzgado Letrado en lo Penal de 15º Turno condenó por un delito continuado de fraude (Art. 160 del Código Penal) a un funcionario del Banco República que modificó el código fuente del software de balances, de tal manera que transfería partidas menores a cuentas de su titularidad.[13] El encausado logró acumular mediante pequeñas fracciones más de U$S 120.000.

---

[11] Sentencia Nº 397 del 16 de Noviembre de 2004 del Tribunal de Apelaciones en lo Penal de 2º Turno.

[12] Sentencia Nº 230 del 11 de Noviembre de 2005 de la Suprema Corte de Justicia.

[13] Sentencia Nº 5 del 4 de Febrero de 2005 del Juzgado Letrado de Primera Instancia en lo Penal de 15º Turno.

La posibilidad de filmar en alta definición utilizando aparatos cada vez más pequeños ha abierto la puerta a que se divulguen imágenes que originalmente fueran captadas para mantener en la intimidad. Esto se ha utilizado como medio de extorsión, amenazas o por pura venganza ante crisis de pareja.

Los bienes jurídicos que se tutelan en estos casos son la imagen, la intimidad y la libertad sexual de la persona afectada por la divulgación. La viralización del contenido puede ocasionar grandes daños a la víctima que busca, más que la condena del culpable, una rápida solución y reparación dando de baja el contenido de la red.[14]

Resulta recomendable que estos delitos, como ocurre en varios de los delitos sexuales de nuestro Código, se persigan únicamente a instancia del ofendido.

Además debe excluirse la responsabilidad de los intermediarios que no tuvieran un rol activo en la publicación. La penalización a los intermediarios que no dieran de baja el contenido, puede conllevar mecanismos de censura privada. Es decir, el miedo a recibir una sanción por material publicado por terceros podría provocar que los intermediarios actuaran como filtro sobre qué y cómo publicar. Además ante una denuncia –por más injustificada que fuera- preferirían dar de baja el contenido para evitar sanciones posteriores, lo que podría lesionar directamente la libertad de expresión, por ejemplo con obras de arte.

---

[14] El fundamento de penalización de las conductas de *Revenge Porn* podría encontrarse en la Convención Interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (conocida como ''Convención de Belem do Pará''), ratificada en Uruguay por la Ley Nº 16.735. Ver (Palazzi, 2016)

La falta de tipificación específica no ha impedido a la jurisprudencia nacional pronunciarse sobre este tipo de conductas. Por Sentencia 214/2015 del Tribunal de Apelaciones Penal de 1º Turno se mantuvo firme el procesamiento contra el imputado por subir al muro de Facebook de su expareja un video donde esta le practicaba sexo oral. Si bien en primera instancia se proceso por un delito de Injuria, el Tribunal modificó la carátula por el de Violencia Privada.[15]

Otro de los tipos penales aplicados en este tipo de casos es el de Exhibición Pornográfica, como aconteció en Canelones, donde se procesó a un individuo por enviar al grupo de WhatsApp de sus amigos un video donde mantenía relaciones sexuales con dos personas más.[16]

Robo o Suplantación de Identidad

Se identifican 3 fases en la comisión de este delito:

- La obtención de información de identidad, mediante ataques externos, ingeniería social, malware, phishing u otras técnicas.

- La posesión y/o puesta a disposición de la información obtenida, lo que incluye la venta a terceros.

- El uso de esa información para cometer un delito, por ejemplo, la estafa.

Este tipo de delitos protege bienes jurídicos como el honor, la privacidad y la propiedad, para los casos en que se busca obtener un beneficio económico por intermedio de la suplantación.

[15] Sentencia Nº 214/2015 del Tribunal de Apelaciones en lo Penal de 1º Turno.

[16] Auto de Procesamiento del 21/04/2015 del Juzgado Letrado de Canelones de 1º Turno.

Sin embargo, las redacciones amplias o ambiguas del tipo pueden provocar amenazas para la libertad de expresión a través de los medios digitales. Prácticas como la parodia o el anonimato podrían ser criminalizadas, pese a ser legítimas por representar una forma de expresión que protege a los emisores de represalias injustificadas. (Relatoría Especial para la Libertad de Expresión, 2013)

Según las Notas Guías del Comité de la Convención de Cibercriminalidad, cada una de las fases del delito de Robo de Identidad pueden ser penadas por los diferentes delitos previstos en la Convención, siempre que se provoque un daño o se utilice para la comisión de otro delito. De esta manera, la previsión de un delito independiente, resultaría innecesaria de existir una norma que introduzca las previsiones de Budapest en el ordenamiento nacional. (Consejo de Europa, 2014)

En caso de entender pertinente su tipificación independiente, el delito debería incluir como elemento objetivo, la ocasión de un daño grave para la víctima o de un perjuicio económico.

Ciberacoso y grooming

El acoso a menores de edad a través de Internet y, en especial a través de redes sociales, supone un fenómeno en aumento y que vulnera bienes jurídicos como la libertad sexual e integridad de la persona. Según cifras del Ministerio del Interior, en el año 2014 se recibieron 450 denuncias por este tipo de delitos, derivando en 19 personas procesadas. (Ministerio del Interior, 2015)

La tipificación de este delito no se encuentra dentro de las recomendaciones del Convenio de Budapest, pero sí del Convenio

del Consejo de Europa sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual.[17]

En Argentina, el Artículo 131 del Código Penal establece a texto expreso el delito de Grooming.[18] Desde la academia y la sociedad civil del vecino país se han señalado diversas críticas sobre la redacción imprecisa y vulneradora de diversos principios penales (Schnidrig, 2016). Dichas críticas son trasladables al proyecto de ley presentado por el Senador Bordaberry en marzo de 2015, basado en el texto vigente en la República Argentina.

Pese a no contar con un tipo específico, la jurisprudencia de nuestro país ha recurrido a los delitos vigentes del Código Penal como los de Violencia Privada[19], Atentado violento al pudor o la Ley de Pornografía Infantil.[20]

---

[17] Artículo 23 Convenio del Consejo de Europa sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual: "Cada parte adoptará las medidas legislativas o de otro tipo que sean necesarias para tipificar como delito el hecho de que un adulto, mediante las tecnologías de la información y la comunicación, proponga un encuentro a un niño (...) con el propósito de obtener cualquier de los delitos tipificados con arreglo al apartado 1.a del artículo 18 o al apartado 1.a del artículo 20, cuando a dicha proposición le hayan seguido actos materiales conducentes a dicho encuentro."

[18] Artículo 131 del Código Penal (República Argentina): "Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma".

[19] https://www.minterior.gub.uy/index.php/2013-06-17-14-41-56/2012-11-13-13-08-52/78-noticias/ultimas-noticias/2587-a-prision-por-publicar-fotos-intimas-de-menor-en-redes-sociales

[20] Sentencia Nº 56 del Juzgado Letrado en lo Penal de 3° turno del 1° de setiembre de 2014 que condena por un delito continuado de Retribución a Menor de Edad Para Ejecutar Actos Sexuales cometido a través de redes sociales.

La Ley No. 18.331 que estableció en nuestro ordenamiento el sistema de protección de datos personales y el proceso de habeas data, no incluyó figuras delictivas contra el tratamiento indebido de datos personales. Algunos países como Argentina y España han optado por seguir el camino de castigar penalmente este tipo de conductas.

La sanción más grave prevista en nuestra ley es la clausura de la base de datos, sanción que la Unidad Reguladora y de Control de Datos Personales aplicó una sola vez en sus ocho años de funcionamiento. [21]

Cualquier modificación del sistema actual debería tener en cuenta el régimen de garantías, derechos y deberes incluidos en la ley mencionada, de forma que su lectura sea coherente y consistente.

---

[21] Sentencia Interlocutoria Nº 13 del 6 de marzo de 2013 del Tribunal de Apelaciones en lo Civil de 1º Turno.

5

SISTEMA PROCESAL

Los desafíos que representan las tecnologías de la información y comunicación al Derecho Penal no se limitan únicamente a la tipificación de nuevos delitos. Factores como la transnacionalidad y dificultades en la identificación de los sujetos responsables, hacen mella en el Proceso Penal.

Un abordaje íntegro del flagelo de los delitos informáticos requiere además de mecanismos de cooperación internacional, capacitación y potestades jurídicas a los diferentes agentes del Estado para perseguir las conductas antijurídicas cometidas por medios informáticos.

El Convenio de Cibercrimen, reconociendo estas dificultades, incluye previsiones sobre la determinación de jurisdicción competente, asistencia mutua entre países, y medidas cautelares como la interceptación y conservación de datos informáticos.

En el informe "Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?" de la OEA y el BID, Uruguay presenta un nivel "Formativo" en las categorías Derecho Procesal de delincuencia cibernética e Investigación Jurídica. Los aspectos evaluados en estas categorías incluyen la capacidad de investigación para procesar las pruebas electrónicas y luchar contra la delincuencia cibernética, incluida la forma de evaluar, obtener y tratar la evidencia digital y utilizar los instrumentos procesales adecuados.

En Uruguay no existen fiscalías o juzgados especializados en la persecución de delitos informáticos. En agosto de 2016, la Resolución 578/2016 de la Fiscalía General de la Nación estableció la creación de un grupo de trabajo para la elaboración de un protocolo de actuación sobre Delitos Informáticos.

A nivel regional, las Reuniones de Ministros de Justicia u otros Ministros, Procuradores o Fiscales Generales de las Américas (REMJA) cuentan con un Grupo de Trabajo para Delitos Informáticos, el cual brinda recomendaciones y permite el intercambio de experiencias.

La iniciativa MERCOSUR Digital intentó generar el marco de cooperación necesario para el desarrollo de capacidades dentro de las que se incluía la persecución de delitos informáticos. Actualmente el programa no se encuentra dentro de los Proyectos en Ejecución del bloque regional. (MERCOSUR, 2016)

El Código del Proceso Penal 2017, introduce dentro de sus previsiones (Artículo 205 y siguientes) las medidas de interceptación de comunicaciones que el Fiscal podrá solicitar en el marco de un proceso penal. Se desplaza así cualquier tipo de incertidumbre sobre la posibilidad de utilizar medidas de vigilancia electrónica en la investigación de cualquier delito, ya que hasta el momento la norma habilitante se encontraba en la Ley 18.494 de Control y Prevención de Lavado de Activos (Art. 5).

A la hora de brindar potestades y herramientas, como la interceptación de comunicaciones, a policía, fiscales y jueces se deben tener en cuenta el respeto por los derechos humanos y el debido proceso. Las TIC's son herramientas y como tales no son por sí mismas valiosas o disvaliosas. Son las conductas de los sujetos las que deben ser objeto de reproche. La regulación ex ante de la herramienta por sí misma, sin tener en cuenta el actuar de la persona podría representar una lesión a un derecho reconocido.

Así por ejemplo, el anonimato que muchas veces es visto desde una perspectiva negativa por obstaculizar las investigaciones y permitir a los delincuentes no dejar rastros, puede ser valioso también como medio para el ejercicio de otros derechos. En este sentido, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha entendido: "(...) los Estados deben evitar la implementación de cualquier medida que restrinja, de manera arbitraria o abusiva, la privacidad de los individuos (artículo 11 de la Convención Americana), entendida en sentido amplio como todo espacio de intimidad y anonimato, libre de amedrentamiento y de represalias, y necesario para que un individuo pueda formarse libremente una opinión y expresar sus ideas así como buscar y recibir información, sin ser forzado a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta" (Relatoría Especial para la Libertad de Expresión, 2013, p. 63).

Otro ejemplo lo constituyen las discusiones en torno a la encriptación o cifrado. En los últimos años gobiernos de diferentes países han intentado establecer requisitos de puertas traseras o backdoors para los fabricantes de dispositivos electrónicos de forma tal que permitan a las autoridades policiales analizar contenido que se encuentra encriptado. Una especie de llave maestra que permita conocer el contenido de cualquier dispositivo.

"Los gobiernos que proponen el acceso de puerta trasera no han demostrado que el uso del cifrado por delincuentes o terroristas constituya una barrera insuperable para los objetivos relacionados con el cumplimiento de la ley"- Afirma el Relator Especial para la Promoción y Protección de la Libertad de Opinión de la ONU- "Además, en base a la tecnología existente, las deficiencias intencionadas menoscaban de forma invariable la seguridad para todos los usuarios de la red, ya que una puerta trasera, aunque haya sido concebida únicamente para permitir el acceso al gobierno, puede ser utilizada por otras entidades no

autorizadas, incluidos otros actores estatales o no estatales. Dado su efecto generalizado e indiscriminado, el acceso de puerta trasera afectaría, de forma desproporcionada, a todos los usuarios de la red" (Kaye, 2015) La explotación de los puntos débiles intencionados torna vulnerable al sistema ante ataques de terceros, incluso si únicamente se tiene la intención de permitir el acceso al gobierno o al órgano judicial.

Las mismas herramientas pueden ser utilizadas para cometer delitos así como para defender derechos humanos o para administrar redes, lo que dificulta tomar decisiones previas y requiere de un especial cuidado. El uso que de ellas se dé va a ser el factor determinante sobre su valoración.

Por otra parte, las comunicaciones electrónicas permiten la recolección masiva de datos, lo cual acompañado de amplios poderes de investigación puede afectar derechos fundamentales de las personas. Las técnicas de vigilancia mediante TIC's pueden pasar inadvertidas completamente, al tiempo que son intrusivas en la vida íntima del individuo.

La retención de datos por parte de las empresas de telecomunicaciones (lo que incluye los metadatos de los usuarios) es aún un tema en debate que no ha logrado el consenso a nivel internacional.[22] Se debe tener en cuenta que establecer la recolección obligatoria y masiva de datos mediante una ley contribuye a la creación de un estado permanente de vigilancia, donde se recoge información de todos en todo momento, invirtiendo así el principio de inocencia. Además estas obligaciones generan importantes costos y riesgos para las

---

[22] No existe un consenso internacional sobre el plazo exigido para la retención por lo que cada país ha optado por definir el periodo a nivel interno, existiendo importantes diferencias: 6 meses: Alemania, Suecia; 12 meses: Brasil, España, Paraguay, Portugal, Reino Unido; 2 años: Australia, México. En 2014 la Corte de Justicia de la Unión Europea invalidó la Directiva de Retención de Datos por atentar contra los derechos fundamentales a la privacidad y la protección de datos personales. (Kapellmann Zafra & Reyes Ampudia, 2014)

operadoras que deben mantener y proteger grandes bases de datos por más tiempo.

Con el fin de lograr un desarrollo equilibrado entre la vigilancia y el derecho a la privacidad en las comunicaciones la comunidad de expertos y organizaciones ha promulgado en 2013 los Principios Internacionales Sobre La Aplicación De Los Derechos Humanos A La Vigilancia De Las Comunicaciones. Estos principios abogan por un análisis de proporcionalidad y necesidad a la hora de establecer normas y mecanismos de vigilancia sobre la población de un país.

6

CONCLUSIONES Y RECOMENDACIONES

La posición de Uruguay como referente en la Sociedad de la Información y la implementación del Gobierno Electrónico, no se condice con las evaluaciones recibidas cuando se habla de delitos informáticos y su persecución. Esta falta ha sido señalada desde diferentes ámbitos lo que ha motivado la presentación de proyectos de ley que penalizan conductas relacionadas con las TICs.

Sin embargo, la normativa penal, sustancial y procedimental, es sólo una de las facetas de un fenómeno más amplio reconocido como Ciberseguridad. El Derecho Penal actúa después de ocurrido el hecho, cuando el daño ya está ocasionado, post facto. Como parte de una estrategia de Ciberseguridad global que ponga el foco en los derechos de los ciudadanos, es preferible la adopción de medidas proactivas, como pueden ser la colaboración entre sector público y sector privado, el desarrollo de personal capacitado, o la difusión de información.

Abordar este problema requiere contar con información a la vista, de forma que se conozca la dimensión del problema. Mejorar las prácticas de transparencia activa y pasiva en materia de seguridad contribuiría a la comprensión y el desarrollo de estudios sobre el tema, logrando así mejores herramientas para la legislación.

Es necesario además contar con un análisis criminológico que permita identificar las características de los autores y las víctimas de este tipo de conductas, creación de cuerpos especializados, la capacitación del personal, la cooperación internacional, los centros de respuesta a incidentes informáticos, y la educación de los usuarios son herramientas fundamentales para prevenir y combatir los daños ocasionados por el cibercrimen.

La redacción de los tipos penales debe ser estricta, sin lugar a ambigüedades. La redacción de las normas penales debe ser lo más clara y precisa que se pueda, evitando los tipos penales en blanco y redundancias que no dejen en claro la conducta referida. Ya sea por impericia o desconocimiento, las personas podrían verse involucradas en algunas de las conductas tipificadas de manera amplia. A modo de limitar las sanciones a quienes actúan fuera del marco de la ley, dolosamente o con conocimiento de causa, y no por simple negligencia o inadvertencia, resulta recomendable incluir elementos objetivos y subjetivos en la redacción de los delitos.

Además se debe tener en cuenta que la redacción de tipos penales amplios puede llevar a englobar conductas socialmente beneficiosas. Actividades de investigación, auditoría o ingeniería inversa resultan en muchas ocasiones en mejoras a los sistemas de seguridad de las organizaciones públicas y privadas, por ejemplo a través de la comunicación de vulnerabilidades o fallas a los administradores. Sin embargo, estas conductas pueden llegar a verse amenazadas o desincentivadas ante la promulgación de delitos como el de Acceso ilícito o Abuso de dispositivos perjudicando en última instancia a los usuarios y organizaciones. La regulación de delitos informáticos no debería dejar de lado esta faceta lo que podría socavar la investigación y desarrollo de mejores medidas de seguridad.

Por su parte, los mecanismos de persecución e investigación deben ser respetuosos con los derechos individuales y no procurar lesionar libertades. El Derecho Procesal debe acompañar las reformas sustanciales que se hagan en este ámbito ya que resulta otro de los pilares fundamentales para la seguridad digital del país.

El Convenio de Budapest es referencia en el mundo entero, incluyendo países de la región latinoamericana, pese a las críticas mencionadas. Los Proyectos presentados hasta el momento en Uruguay han adoptado este intsrumento europeo como fuente de inspiración. Si se eligiera recorrer el camino de adaptar las normas nacionales a lo dispuesto por el Consejo de Europa, se deben tener en cuenta determinados aspectos y evitar la simple transposición de normas. "Armonización" no quiere decir "Idéntico". Lo que se requiere es complementariedad que permita a los mecanismos de cumplimiento de la Ley trabajar eficientemente, respetando las diferencias nacionales y regionales. (Clough, 2014)

Adherir al Convenio no significa trasladar automáticamente un conjunto de normas rígidas que no puedan ser modificadas. Dentro de cada uno de los tipos, la redacción de Budapest otorga un margen de elección a los legisladores de cada país, de forma de volver más o menos punitiva la norma interna. Algunos ejemplos de ello son la inclusión del elemento objetivo de "daño grave" (Art. 4) o del elemento subjetivo "con la intención de obtener datos informáticos" (Art. 1). Una posición garantista y protectora de los derechos humanos, implica adoptar estas previsiones objetivas o subjetivas dentro de los tipos penales nacionales. De esta manera se limita el poder punitivo del Estado en materia penal, que no se debe olvidar, funciona como ultima ratio, cuando no existen otras soluciones posibles.

7

BIBLIOGRAFÍA

Acurio Del Pino, S., s.f. Delitos Informáticos: Generalidades. Available at: http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aller, G., 2010. Criterios de imputación y punitivos en los delitos informáticos. Anuario de Derecho Informático, Issue 11, pp. 39-59.

Anon., 2007. Delito e Informática: algunos aspectos. Bilbao: Universidad de Deusto.

Anon., 2011. Anonymous atacaría webs del gobierno uruguayo. Available at: http://www.180.com.uy/articulo/21493_Anonymous-atacaria-webs-del-gobierno-uruguayo [Último acceso: 06 02 2017].

Anon., 2016. Destruyendo el sistema bancario. Available at: https://elcuervo.net/blog/destruyendo-el-sistema-bancario/ [Último acceso: 10 03 2017].

Asociación por los Derechos Civiles (ADC), 2016. Ciberseguridad en la era de la vigilancia masiva, Buenos Aires: s.n.

Bauzá, M., 2012. Criminalidad informática: Reto crítico y abierto. Revista de Legislación Uruguaya, 3(7), p. 13.

Bertoni, E., Lanza, E., Mas, M. & Torres, N., 2012. Seguridad Nacional y Acceso a la Información en América Latina: Estado de situación y desafíos, Montevideo: Open Society Foundation.

Camps, P., 2016. Ciberdefensa y ciberseguridad: nuevas amenazas a la seguridad nacional, estructuras nacionales de ciberdefensa, estrategias de ciberseguridad y cooperación interagencias en este ámbito.. [En línea] Available at: http://www.calen.gub.uy/pdf/investigacion/2016-1-Ciberseguridad-Camps.pdf [Último acceso: 03 12 2016].

Certuy, 2016. Correo fraudulento que simula ser de DGI. Available at: https://www.cert.uy/inicio/novedades/alertas_y_vulnerabilidades/correo+fraudulento+que+simula+ser+de+dgi [Último acceso: 06 02 2017].

Chertoff, M. & Simon, T., 2015. The Impact of the Dark Web on Internet Governance and Cyber Security , Ontario: Chatam House.

Clough, J., 2014. A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. Monash University Law Review, 3(40), pp. 698-736.

Consejo de Europa, 2014. T-CY GUIDANCES NOTES. Available at: https://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/TCY(2013)29rev_GN%20compilation_v3.pdf [Último acceso: 16 08 2016].

Consejo de Europa, s.f. Informe Explicativo del Convenio sobre Ciberdelincuencia (STE núm. 285), s.l.: s.n.

de La Chapelle, B. & Fehlinger, P., 2016. Jurisdiction on the Internet, s.l.: Global Commission on Internet Governance.

Derechos Digitales, APC, Coding Rights, 2015. Latin América in a Glimpse, s.l.: s.n.

di Piero, C., 2013. El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio. InDret, 07.Issue 3.

Elías Puelles, R., 2014. Luces y sombras en la lucha contra la delicuencia informática en el Perú, Lima: s.n.

Fundación Karisma, 2016. Declaración sobre Seguridad Digital en América Latina. Available at: https://karisma.org.co/declaracion-sobre-seguridad-digital-en-america-latina/ [Último acceso: 12 08 2016].

Gercke, M., 2009. UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES. [En línea] Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf [Último acceso: 6 02 2017].

Green, N. & Rossini, C., 2015. Cyber Security and Human Rights, Washington: s.n.

Hosein, G. & Yalamova, M.-M., 2013. International Co-Operation and Intercultural Relations: Reconciling the Security and Privacy Agendas. En: Ethical Governance of Emerging Technologies Development. s.l.:s.n., p. 54.

Kapellmann Zafra, D. & Reyes Ampudia, B., 2014. Retención y Privacidad de Datos: Algunas Lecciones Derivadas de las Diversas Prácticas Internacionales , s.l.: The Social Intelligence Unit.

Kaye, D., 2015. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Nueva York: s.n.

La República Perú, 2013. Ley de Delitos Informáticos: estos son sus riesgos y peligros. La República, 22 10.

Landa Durán, G., 2007. Los delitos informáticos en el Derecho penal de México y España. Revista del Instituto de la Judicatura Federal, Issue 24, pp. 233-256.

Langón, M., 2016. Código Penal y Leyes Complementarias Comentados. Montevideo: Universidad de Montevideo.

Machado, R., 2014. Fuga de datos y responsabilidad empresarial. Diario El País, 3 10.

Martínez, M., s.f. Delitos Informáticos ¿El derecho positivo uruguayo tiene respuestas adecuadas?. Available at: http://www.lenspacareu.com.uy/v1/data/La_Problematica_de_los_Delitos_Informaticos_-__Breve_vision_del_tema.pdf

Matellanes Rodríguez, N., 2008. Vías para la tipificación del acceso ilegal a los sistemas informáticos. Revista Penal, 07, Issue 22, pp. 50-68.

Maurer, T. & Morgus, R., 2014. Compilation of Existing Cybersecurity and Information Security Related Definitions , s.l.: s.n.

MERCOSUR, 2016. Proyectos en ejecución. [En línea] Available at: http://www.mercosur.int/innovaportal/v/6810/7/innova.front/proyectos-en-ejecucion

Ministerio del Interior, 2015. La Policía monitorea aumento de casos de ciberacoso y realiza recomendaciones. [En línea] Available at: https://www.minterior.gub.uy/index.php?option=com_content&view=article&id=2490 [Último acceso: 06 02 2017].

Montserrat Sánchez-Escribano, M., 2014. Panorama normativo supranacional del delito de acceso ilícito a un sistema

informático. En: Investigaciones en ciencias jurídicas: desafíos actuales del derecho. Málaga: s.n.

Nyst, C., 2016. Travel Guide to the Digital World: Cybersecurity Policy for Human Rights Defenders, Londres: s.n.

OEA, BID, 2016. Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, Washington: s.n.

ONU, 2016. UNITED NATIONS E-GOVERNMENT SURVEY 2016. Available at: http://workspace.unpan.org/sites/Internet/Documents/UNPAN96407.pdf

Organización de Estados Americanos, 2013. Documento Explicativo del Proyecto Ley Modelo para Facilitar e Incentivar la denuncia de actos de corrpución y proteger a sus denunciantes. Available at: http://www.oas.org/juridico/ley_explicativo_prot.pdf [Último acceso: 12 03 2017].

Palazzi, P., 2016. Difusión no autorizada de imágenes íntimas (Revenge Porn). El Derecho, 03.

Pecoy, M., 2012. Delitos Informáticos. Montevideo: Universidad de Montevideo.

Prasad, T., 2014. Ethical Hacking and Types of Hackers. International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), Noviembre.11(2).

Red de Gobierno Abierto, 2014. Declaración sobre el proyecto de ley de Delitos Informáticos. Available at: http://rga.uy/declaracion-sobre-el-proyecto-de-ley-de-delitos-informaticos/ [Último acceso: 05 02 2017].

Relatoría Especial para la Libertad de Expresión, 2013. Libertad de expresión e Internet, Washington: s.n.

Resolución 578/2016, 2016. Fiscalía General de la Nación. Available at: http://www.fiscalia.gub.uy/innovaportal/file/866/1/creacion-comisiones---protocolos-de-actuacion-1.pdf [Último acceso: 14 Marzo 2017].

Reuters, 2016. Pakistan passes controversial cyber-crime law. Available at: http://www.reuters.com/article/us-pakistan-internet-idUSKCN10N0ST

Rueda Martín, M. Á., 2010. Los ataques contra los sistemas informáticos: Conductas de Hacking. Cuestiones político-criminales. En: La adaptación del Derecho Penal al desarrollo social y tecnológico. s.l.:Comares, pp. 347-379.

Schnidrig, D., 2016. El Delito de 'Grooming' en la legislación penal actual y proyectada en Argentina, Buenos Aires: Universidad de Palermo.

Scrollini, F., Tuduri, A. & Rodríguez, K., 2016. Vigilancia Estatal de las Comunicaciones y Protección de los Derechos Fundamentales en Uruguay, Montevideo: Electronic Frontier Foundation.

Tellez Valdez, J., 1998. Delitos Informáticos. En: Derecho Informático. Ciudad de México: UNAM, pp. 103-107.

UIT, 2014. Global Cybersecurity Agenda, Ginebra: UIT.

UIT, 2015. Índice mundial de ciberseguridad y perfiles de bienestar, s.l.: s.n.

Viega, M. J. & Carnikián, F., 2010. Respuestas a los delitos informáticos: su visión desde la privacidad y la seguridad de la información. Cartagena de Indias, s.n.

ANEXO

MINISTERIO DEL INTERIOR
DEPARTAMENTO DE ASESORIA JURIDICA
ASESORIA LETRADA

Dictamen N° 883/2016 Expediente 2016-4-1-0011812.-

Montevideo, 16 de agosto de 2016.-

SEÑORA DIRECTOR DEL DEPARTAMENTO DE ASESORIA JURIDICA.-

I – OBJETO

Vienen a conocimiento de esta Repartición las presentes actuaciones con la solicitud presentada por el Señor Matias Jackson, quien requiere información en formato electrónico respecto a delitos informáticos (Fojas 3).-

II – ANTECEDENTES

El peticionante requiere se detalle:

- Estadísticas de delitos informáticos en Uruguay en los últimos 10 años desglosadas por año.

- Cantidad de denuncias efectuadas ante el Departamento de Delitos Informáticos de la Policía en los últimos 10 años, desglosadas por año.

- Cantidad de policías asignados al Departamento de Delitos Informáticos y Tecnológicos (actualmente).-

III – ANALISIS

El artículo 3 de la Ley 18.381 de fecha 17/10/08 dispone que el acceso a la información pública es un derecho de todas las personas y se ejerce sin necesidad de justificar las razones por las que se solicita la información.-

El artículo 8 dispone que las excepciones a la información pública serán de interpretación estricta y comprenderán aquellas definidas como secretas por la ley y las que se definan como de carácter reservado y confidencial. Los artículos 9 y 10 definen los casos en que la información se considera reservada y confidencial respectivamente.

No podrá accederse a brindar la información solicitada siempre que los archivos mencionados se relacionen con alguna de las hipótesis de información reservada reguladas expresamente, entre otras se señalan:

- Resolución Ministerial de fecha 20/07/12: Información y documentación que involucre el ejercicio de actividad policial, en particular toda aquella relativa a hechos y

personas que sea recabada y tratada con finalidad del mantenimiento y preservación del orden público, así como para prevención y represión del delito.

- Resolución Ministerial de fecha 30/07/12: Información y documentación relativa a la estructura edilicia y ubicación de las distintas dependencias del Ministerio del Interior entre los que están comprendidas esta Secretaría de Estado, Direcciones Nacionales, Jefaturas Departamentales, Seccionales Policiales, viviendas y toda dependencia de las mismas, en particular en lo relativo a las vías de acceso, cantidad y distribución de personal policial que presta servicios en dichos locales, asignación del trabajo y directivas para el mismo, así como respecto de los móviles del servicio, su distribución y los materiales e insumos que se utilicen.

Asimismo se destaca que no debe concederse acceso a los archivos que contengan información que encuadraría dentro de la categoría de información confidencial prevista por el artículo 10 de la citada ley.

En tanto, tampoco podría concederse acceso a la documentación que se encuentra protegida por la Ley de Protección de Datos Personales, Número 18.331, del 06/08/2008.-

La misma señala: "*Artículo 3: Ámbito objetivo.- El régimen de la presente ley será de aplicación a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.*

No será de aplicación a las siguientes bases de datos: A) A las mantenidas por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. B) Las que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito. C) A las bases de datos creadas y reguladas por leyes especiales.

Artículo 25: Base de datos correspondientes a las Fuerzas Armadas, Organismos Policiales o de Inteligencia.- Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de las fuerzas armadas, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichas bases de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.

El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos supuestos y categoría

de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Las bases de datos, en tales casos, deberán ser específicas y establecidas al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad.

Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Artículo 26: Excepciones a los derechos de acceso, rectificación y cancelación.- Los responsables de las bases de datos que contengan los datos a que se refieren los incisos segundo y tercero del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

Los responsables de las bases de datos de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el inciso anterior cuando el mismo obstaculice las actuaciones administrativas tendientes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el titular del dato esté siendo objeto de actuaciones inspectivas.

El titular del dato al que se deniegue total o parcialmente el ejercicio de los derechos mencionados en los incisos anteriores podrá ponerlo en conocimiento del Órgano de Control, quien deberá asegurarse de la procedencia o improcedencia de la denegación."

IV – CONCLUSIONES

En la medida de que, la dictaminante desconoce si este Ministerio lleva un registro similar al solicitado, estima oportuno indicar que correspondería acceder a lo peticionado, siempre que, la información que los mismos contengan, no haya sido declarada como información reservada o confidencial por parte del Jerarca y siempre que exista el registro mencionado.-

Se debe tener en cuenta lo dispuesto que por el art. 14 de la Ley 18.381 "*La solicitud de acceso a la información no implica la obligación de los sujetos obligados a crear o producir información que no dispongan o no tengan obligación de contar al momento de efectuarse el pedido....*"

Asimismo, la información debe brindarse dentro de los plazos establecidos por el artículo 15 de la Ley: "*Cualquier persona física o jurídica podrá formular la petición de acceso a la información en poder de los sujetos obligados. Ante la petición*

formulada por el interesado, el organismo requerido está obligado a permitir el acceso o, si es posible, contestar la consulta en el momento en que sea solicitado. En caso contrario tendrá un plazo máximo de veinte días hábiles para permitir o negar el acceso o contestar la consulta.

El plazo podrá prorrogarse, con razones fundadas y por escrito, por otros veinte días hábiles si median circunstancias excepcionales".-

Sin otro particular, saluda a Usted atentamente,

Cabo (PA)

Dra. María Cecilia Alvarez Marques

Abogada

.DZ F1

MINISTERIO DEL INTERIOR
DIRECCIÓN DE LA POLICÍA NACIONAL

Oficio N° 533/16 - ML/AS/mm

Montevideo, 23 de setiembre de 2016.

Señor Director de la D.G.L.C.C.O. e INTERPOL
Crio. Gral. Carlos DEL PUERTO:

A los efectos de evacuar información solicitada a ésta al bajo el amparo de la Ley 18.381, se solicita informe en carácter de URGENTE y en forma numérica:

1) Estadísticas de Delitos Informáticos en Uruguay en los últimos 10 años, desglosadas por año.

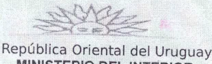
2) Cantidad de denuncias efectuadas ante el Departamento de Delitos Informáticos de la Policía en los últimos 10 años, desglosadas por año.

Saluda a Usted atentamente.

El Director de la Policía Nacional
Crio. Gral. ®
Mario R. LAYERA

MINISTERIO DEL INTERIOR
D.G.L.C.C.O. E INTERPOL
Secretaría General
Montevideo, 27 SET. 2017 N° Registro 6505
Pase a D Ct
☐ Informar ☐ Notificar
☒ A sus efectos ☐ Registro
☒ Para derivar ☐ Realizar RED NACIONAL
☒ Cumplido, vuelva ☐ Cumplido, Archívese

DIRECTOR DE LA D.G.L.C.C.O. e INTERPOL
COMISARIO GENERAL
Carlos del PUERTO RODRIGUEZ


República Oriental del Uruguay
MINISTERIO DEL INTERIOR

DIRECCION GENERAL de LUCHA CONTRA el CRIMEN ORGANIZADO e INTERPOL
DIVISION CRIMEN ORGANIZADO
DPTO. DE INVESTIGACIONES COMPLEJAS.



INFORME : 286 /16WAR
REF: Estadística y cantidad de denuncia en la Sección de Delitos Tecnológicos.-.-.-.-..-.-.

Montevideo, 04 de Octubre del 2016.-

SR. JEFE DEL DPTO. DE INVESTIGACIONES COMPLEJAS.

Por medio del presente cúmpleme informar a usted, que se recibió en este Depto Oficio 533/16 de la Dirección de la Policía Nacional en donde se solicita de forma URGENTE y en forma numérica:

a- Estadísticas de Delitos Informáticos en Uruguay en los últimos 10 años desglosadas por año.

b- Cantidad de denuncias efectuadas ante el Departamento de Delitos Informáticos de la Policía en los últimos 10 años desglosadas por año.

Por tal motivo y por lo anteriormente solicitado, se informa que:

1. Esta Sección no cuenta con estadística de Delitos Informáticos , denunciados en todo el país, debido a que solo se lleva registro de las denuncias presentadas en esta Sección de Delitos Tecnológicos.

   a- Por otro lado se informa que las diferentes unidades policiales de todo el país, ingresan las novedades al S.G.S.P que guardan relación con las competencias de Delitos Tecnológicos, de la siguiente forma como por ejemplo, Difusión de videos íntimos **(con la tipificación de VIOLENCIA PRIVADA**), amenazas vía facebook **(AMENAZAS)**, estafas a través de mercado libre o en internet **(ESTAFAS)**, hurto de notebook (HURTO EN CASA DE FAMILIA,) siendo campos que ya están predeterminados por el

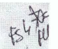
f33

Sistema e ingresando la novedad con diferentes tipificación de delitos, siendo así difícil establecer la cantidad de denuncias efectuadas en el S.G.S.P a nivel de todo el pais .

b- La sección de Delitos Informáticos la que así, se llamaba originariamente fue creada en el año 2005, y dependía del Departamento de Delitos Complejos de la Dirección de Investigaciones de la Jefatura de Montevideo (debido a la reestructura efectuada en su momento en la Jefatura de Policía de Montevideo, no se posee en esta sección datos de esa época, en cuanto al volumen y cantidad de denuncias que se trabajaba en dicha sección, datos que deberían estar en la Jefatura de Policía de Montevideo), luego en el año 2011 la sección cambia de nombre a Delitos Tecnológicos y paso a la órbita de la Dirección General de Lucha Contra el Crimen Organizado e Interpol del cual si hay registro de denuncias.

2. Registro de denuncias de la Sección de delitos Tecnológicos.

	AÑO 2012	AÑO 2013	AÑO 2014	AÑO 2015	AÑO 2016
DENUNCIAS	DENUNCIAS 170	DENUCIAS 250	DENUNCIAS 330	DENUNCIAS 420	DENUNCIAS 450
REPORTES DE WASHINGTON		400 Reportes Reportes de CYBERTIPLINE -Explotación Sexual en LINEA	637 Reportes	750 Reportes.	910 Reportes. Interpol EEUU infoma que en los Reportes de CYBERTIPLINE un usuario estaria difundiendo imágenes de menores con contenidos sexual.



* **Los Reportes de CYBERTIPLINE, que Son.?:** Las redes sociales en EEUU están obligadas a reportar a la policía de su país ante cualquier representación por cualquier medio de un niño involucrado en actividades sexuales explicitas reales o simuladas. A través de las Ips generadas en la redes se le informa en formato de Reportes a interpol, que iPs de Uruguay estarían difundiendo imágenes con contenido de menores de edad (imágenes o videos) una vez en esta oficinas se realizan la investigaciones pertinentes a fin de determinar si dicha información se ajustan a le Ley 17,815 del año 2004 ..

3. También se informa, que la sección de Delitos Tecnológicos no es la única oficina policial que trabaja en esta Dirección General denuncias en donde se utiliza Internet y la alta tecnología como forma de delinquir, delitos como ser, clonación de tarjetas y estafas electrónicas, desconociendo el volumen de denuncias efectuadas en dicho Depto.

Siendo todo cuanto tengo que informarle.

Saluda a Usted atentamente.-

EL ENCARGADO DE LA SECCION DE DELITOS TECNOLOGICOS

OF. PPAL: ______________

Winston Rodriguez.-